Oracle® Communications Billing and Revenue Management

Elastic Charging Engine 11.3 Security Guide

Release 7.5

E70770-01

April 2016

Oracle Communications Billing and Revenue Management Elastic Charging Engine 11.3 Security Guide, Release 7.5

E70770-01

Contents

Preface v

Audience v
Documentation Accessibility v
Related Documents v
Accessing Oracle Communications Documentation v

1 ECE Security Overview

Basic Security Considerations 1-1
Overview of ECE Security 1-1
Understanding the ECE Environment 1-2
Oracle Coherence Security 1-2
Oracle NoSQL Database Security 1-2
Security Considerations for Developers 1-2

2 Performing a Secure ECE Installation

Performing a Secure ECE Installation 2-1
About Cluster Security 2-2
About the Keystore Files and SSL Considerations 2-2
About Trusted Host Information 2-3
About JMX Security 2-3
Post-Installation Security Tasks 2-4

3 Implementing ECE Security

About Managing ECE Security 3-1

Preface

This guide provides guidelines and recommendations for setting up Oracle Communications Billing and Revenue Management (BRM) Elastic Charging Engine (ECE) and its components in a secure configuration.

Audience

This document is intended for system administrators, application administrators, and developers.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` or visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` if you are hearing impaired.

Related Documents

For more information, see the following documents in the Oracle Communications Elastic Charging Engine Release 7.5 documentation set and Oracle Coherence Release 3.7 documentation set:

- *Oracle Communications Elastic Charging Engine Installation Guide*
- *Oracle Communications Elastic Charging Engine System Administrator's Guide*
- *Oracle Coherence Management Guide*

In addition, see the *Oracle NoSQL Database Administrator's Guide*.

Accessing Oracle Communications Documentation

Product documentation is located on Oracle Help Center:

- `http://docs.oracle.com`

1

ECE Security Overview

This chapter provides a high-level overview of security for Oracle Communications Billing and Revenue Management (BRM) Elastic Charging Engine (ECE).

Basic Security Considerations

The following principles are fundamental to using any application securely:

- Keep software up to date. This includes the latest product release and any patches that apply to it.
- Keep up to date on security information. Oracle regularly issues security-related patch updates and security alerts. You must install all security patches as soon as possible. See the "Critical Patch Updates and Security Alerts" Web site:

  `http://www.oracle.com/technetwork/topics/security/alerts-086861.html`
- Limit privileges as much as possible. Users should be given only the access necessary to perform their work. User privileges should be reviewed periodically to determine relevance to current work requirements.
- Monitor system activity. Establish who should access which system components, and how often, and monitor those components.
- Install software securely. For example, use firewalls and secure passwords. See "Performing a Secure ECE Installation" for more information.
- Learn about and use the ECE security features. See the discussion of security in *ECE System Administrator's Guide* for more information.
- Use secure development practices. For example, take advantage of existing security functionality instead of creating your own application security. See "Security Considerations for Developers" for more information.
- Avoid using the option to have an application remember passwords for admin logins and passwords. For example, do not select the **Remember Password** check box in a login screen.
- Apply the latest patch set for JDK to ensure that your running JDK has the latest security fixes.

Overview of ECE Security

Access to ECE files is controlled by creating user accounts and groups and granting specific permissions. The file permissions are granted using UNIX commands in a UNIX shell. Once you have created user accounts and groups and set permissions, users can use ECC to manage ECE files. ECC requires that you set up a password-less

SSH. You use the ECE user, a UNIX account, for setting up password-less SSH. See the discussion about managing security in *BRM Elastic Charging Engine System Administrator's Guide* for information about the ECE user.

Understanding the ECE Environment

When planning your ECE implementation, consider the following:

- Which resources need to be protected? For example:
  - You need to protect customer data, such as customer balance information.
  - You need to protect system components from being disabled by external attacks or intentional system overloads.
- Who are you protecting data from?

  For example, you need to protect your subscribers' data from other subscribers, but someone in your organization might need to access that data to manage it. You can analyze your workflows to determine who needs access to the data; for example, it is possible that a system administrator can manage your system components without needing to access the system data.
- What will happen if protections on strategic resources fail?

  In some cases, a fault in your security scheme is nothing more than an inconvenience. In other cases, a fault might cause great damage to you or your customers. Understanding the security ramifications of each resource will help you protect it properly.

Oracle Coherence Security

To restrict access to the ECE Coherence cluster, you must set up an authorized hosts list. You can optionally enable SSL for intra-cluster communication, in which case you must also enable Well Known Addresses (WKA). See the information about managing security in *BRM Elastic Charging Engine System Administrator's Guide*.

Oracle NoSQL Database Security

Access to the KVStore and its data is performed in two different ways. Access to data is possible through the Java API. Administrative access is performed by using a command line interface or a browser-based graphical user interface. System administrators use these interfaces to perform the few administrative actions that are required by Oracle NoSQL Database. You can also monitor the store using these interfaces.

Oracle NoSQL Database is intended to be installed in a secure location where physical and network access to the store is restricted to trusted users. For this reason, Oracle NoSQL Database's security model is designed to prevent accidental access to the data. It is not designed to prevent malicious access or denial-of-service attacks.

Security Considerations for Developers

ECE requires that all Java processes that join its cluster have a correct set of configuration settings. When using the ECE secure mode, having the correct Coherence properties is not sufficient to join the cluster. Any direct access to Coherence APIs should not be used by developers engaged in writing any extensions of plug-ins to ECE. They must use the Spring and Template framework provided by

ECE. Any direct access to Coherence resources including its caches will throw security exceptions.

2

Performing a Secure ECE Installation

This chapter provides instructions for installing a secure Oracle Communications Billing and Revenue Management (BRM) Elastic Charging Engine (ECE) system and covers security-related deployment issues for each installed component of ECE.

ECE should be deployed into a secured environment; for example,

- ECE is deployed in a closed networked environment in which any public access to the network is denied.
- All ECE hosts are ideally connected to a single switch or in a parallel switch configuration.
- No external processes are run on the hosts running ECE and its constituents.
- Access to the ECE infrastructure is restricted.

ECE security can be further hardened by following the instructions in this chapter.

See *BRM Elastic Charging Engine Installation Guide* for information about installing ECE.

Performing a Secure ECE Installation

By default, ECE is installed in a secure mode. ECE uses security measures such as cluster security and host authorization.

When you install ECE, you are prompted to select your preferred security configuration, such as whether to enable secure socket layer (SSL). Based on the security configuration you select, ECE sets parameters in the relevant Oracle Coherence and ECE configuration files for enabling the following security levels:

- **JMX security**. Clients require a JMX user name and password to connect to ECE JMX Management servers. For example, Elastic Charging Controller (ECC) can use a JMX user name and password to be authenticated to log in to the cluster.
- **Authorized host list**. A process that joins the Coherence cluster has access to ECE services only if it is running on a host defined in the authorized hosts list.
- **Coherence node authentication**. ECE nodes are required to authenticate themselves when trying to join the Coherence cluster. The node credentials are stored in a key store file that must be deployed on the ECE nodes.
- **SSL encryption** (intra-cluster communication). Communication across ECE nodes in the Coherence cluster is encrypted.
- **BRM SSL security authentication.** Communication between ECE and BRM through BRM Gateway is encrypted.

- **PDC SSL security authentication.** Communication between ECE and Pricing Design Center (PDC) is encrypted.
- **EM Gateway SSL security authentication.** Communication between BRM and ECE through External Manager (EM) Gateway is encrypted.

About Cluster Security

ECE uses a file based credentials store or a keystore to keep node credentials that are required to join the cluster and that are used for enabling encryption of cluster communication. The keystore is in the *ECE_Home***/oceceserver/config/server.jks** file. Though the ECE installer creates a **server.jks** file, you can create your own as well if required. If you create a JKS file of your own, make sure it has very limited permissions so that unauthorized access is not allowed. ECE creates another keystore file, **keystore.jks**, under the *ECE_Home***/oceceserver/config** directory which stores symmetric keys to encrypt passwords required to connect to boundary systems such as Oracle Communications Billing and Revenue Management (BRM) and Oracle Communications Pricing Design Center (PDC).

ECE bundles a **jmxremote.password** password file in the *ECE_Home***/oceceserver/config** directory. The **jmxremote.password** file contains the boundary system password which is used to read the **keystore.jks**. Reading the **keystore.jks** is required for extracting a symmetric key that enables encryption and decryption of passwords for JMS notification services. See the discussion about managing external application passwords in *BRM Elastic Charging Engine System Administrator's Guide* for information about ECE clients that use the **jmxremote.password** file for decrypting passwords.

When you install ECE, you enter the following information:

- The account alias for Coherence cluster security
- The key password for Coherence cluster security (the password for the alias)
- The key password for the boundary system alias
- The password for accessing the keystore (the certificate store password)
- DName details

  The DName value specifies the authorization of users for what they can do regarding cluster security.

  The DName is used for authorization as defined in *ECE_Home***/oceceserver/config/permissions.xml**.

See *BRM Elastic Charging Engine Installation Guide* for more information.

About the Keystore Files and SSL Considerations

ECE maintains the following keystore files:

- **server.jks**

  This file stores credentials for cluster node authentication details. It is also used for encrypting intra-cluster communication over SSL.

- **keystore.jks**

  This file stores symmetric keys for boundary system password encryption.

Key and store passwords for SSL are stored by default in the *ECE_Home***/oceceserver/config/charging-coherence-override-secure-prod.xml** file. These can, however, be overridden by defining their respective system properties in the *ECE_Home*/**oceceserver/config/defaultTuningProfile.properties** file.

> **Important:** Oracle strongly recommends not overriding the default *ECE_Home*/**oceceserver/config/charging-coherence-override-secure-prod.xml** file.

Installation Settings when SSL Is Enabled

When you select the SSL options during installation, the following settings are set:

- In *ECE_Home*/**oceceserver/config/ece.properties**:
  - tangosol.coherence.override=charging-cache-config-secure-prod.xml
  - the WKA list in the **charging-cache-config-secure-prod.xml** file

    This should contain the WKA host list provided during the installation.
- In *ECE_Home*/**oceceserver/config/charging-coherence-override-secure-prod.xml**:
  - -Dtangosol.coherence.ssl.keypassword=*keypassword*
  - -Dtangosol.coherence.ssl.storepassword=*storepassword*

  where *keypassword* and *storepassword* are the key and store passwords given during the installation.

About Trusted Host Information

ECE caches contain your subscribers' data. To restrict access to this data, you must specify the machines or processes that you trust and allow to be part of the cluster.

Obtain the IP addresses or host names of all machines or processes that are allowed to access the cluster. Trusted hosts include all of the server machines across which the Coherence cluster is deployed and any other machine that is to be part of the cluster. Include the server machine that runs the Elastic Charging Controller (ECC), and if you use Oracle Enterprise Manager, include the JMX client host running it.

See *BRM Elastic Charging Engine Installation Guide* for more information.

About JMX Security

JMX can be secured by setting the following system parameters:

- In *ECE_Home*/**oceceserver/config/ece.properties**:

  com.sun.management.jmxremote.authenticate=true
- In *ECE_Home*/**oceceserver/config/defaultTuningProfile.properties**:

  -Dcom.sun.management.jmxremote.password.file=../config/jmxremote.password

The file permission of **jmxremote.password** must be set to **400**; otherwise, Elastic Charging Server nodes will not start up.

JMX security is based on Java's standard guidelines as documented at:

`http://docs.oracle.com/javase/1.5.0/docs/guide/management/agent.html`

ECE bundles a **jmxremote.password** password file in the *ECE_Home*/**oceceserver/config** directory and contains two default accounts for JMX credentials as defined in *JRE_HOME*/**lib/management/jmxremote.password.template**:

- monitorRole with read-only permissions
- controlRole with read and write permissions

Passwords for these two accounts can be set in the **jmxremote.password** file bundled in *ECE_Home*/**oceceserver/config**. If more accounts are to be added, then those accounts should be added in the **jmxremote.password** file as well. Refer to the following document for information about setting up authorizations for the new accounts:

`http://docs.oracle.com/javase/1.5.0/docs/guide/management/agent.html`

As the JMX passwords are human readable in the **jmxremote.password**, the file permission must be set to **400**.

> **Note:** The **jmxremote.password** file is used for more than JMX. This file is also used for storing passwords required to authenticate cluster nodes and required to encrypt and decrypt passwords for JMS notification services. See the discussion about managing external application passwords in *BRM Elastic Charging Engine System Administrator's Guide* for more information.

All of the Elastic Charging Controller (ECC) shell commands are JMX aware: if JMX is made secure, you must provide a user name and password with the command that starts ECE services.

If JMX is secured, commands like **start server** or starting a single node, such as **start ecs1**, **start pricingLoader**, **start configLoader**, and so on must provide a user name and password. For example:

```
start server username=controlRole password=password_as_defined
```

In secured mode, it is recommended to use the ECC shell in an interactive mode (all commands are run within the shell and not as arguments to the ECC script). The ECC command sets the file permissions of the file that saves the history of the commands executed to **600**. This protects unauthorized access to old commands to retrieve passwords typed in the command line.

In applications such as JConsole, jVisualVM, or other JMX client applications, the user name and password must be specified in their respective consoles when a connection is made.

Post-Installation Security Tasks

For the most part, the Oracle Universal Installer requests you to enter security information that takes care of post-installation steps typically required for security.

After installation, verify the following in the *ECE_Home*/**ocecesserver/config/permissions.xml** file:

- The **principal** section has the same DName information as was defined during the installation process for creating the **server.jks** file.
- A complete access to all resources is allowed for an authenticated user.

- If the **secure.access.name** system property is set, the **tangosol.coherence.security** system property must be set to **true**. If the **tangosol.coherence.secuity** system property is set to **false**, the **secure.access.name** system property should not be set.

3

Implementing ECE Security

This chapter provides an overview of the security mechanisms offered by Oracle Communications Billing and Revenue Management (BRM) Elastic Charging Engine (ECE). For complete instructions about implementing ECE security mechanisms, see *BRM Elastic Charging Engine System Administrator's Guide*.

About Managing ECE Security

To manage ECE security, you perform the following tasks:

- Set up user accounts and user groups, and grant permissions. After you have created user groups and set permissions, users can log in to the system and use ECE and manage the ECE cluster.

  You can assign permissions for users who run and manage ECE processes, manage rated event files, and manage the ECE file systems. Restrict permissions as much as possible. You may choose to create either a single administrative user with all permissions who runs ECE core processes and manages the rated event files and other directories, or create multiple users with specific permissions to carry out these tasks.

  See *BRM Elastic Charging Engine System Administrator's Guide* for a list of the files that you need to restrict access to.

- Manage passwords. UNIX accounts protected by passwords must be created for ECC. Besides the UNIX accounts, you need to create non-UNIX accounts to access external applications like Oracle Communications Billing and Revenue Management (BRM) and Oracle Communications Pricing Design Center (PDC). BRM and PDC are used to load customer and pricing data respectively into ECE. For secure communication between ECE and these systems, credentials stored in ECE are encrypted and stored in the keystore (the **keystore.jks** file).
- Set up cluster security. To restrict access to the ECE Coherence cluster, you must set up an authorized hosts list. You can optionally enable SSL for intra-cluster communication, in which case you must also enable Well Known Addresses (WKA).
- Set up passwordless Secure Shell SSH between driver and server machines. You must set up passwordless SSH between driver and server machines for ECC to work. Passwordless SSH allows servers to connect to the driver and synchronize ECE files.